

DIALOG(R) File 347:JAPIO
(c) 2006 JPO & JAPIO. All rts. reserv.

07813994 **Image available**
PRINTER, INFORMATION PROCESSOR, PRINT SERVER, CONTROL METHOD FOR PRINTER
AND PRINT SYSTEM AND INFORMATION PROCESSING METHOD

PUB. NO.: 2003-308194 [JP 2003308194 A]
PUBLISHED: October 31, 2003 (20031031)
INVENTOR(s): TAKAGI YOSHIHIRO
APPLICANT(s): CANON INC
APPL. NO.: 2002-113629 [JP 2002113629]
FILED: April 16, 2002 (20020416)
INTL CLASS: G06F-003/12; B41J-005/30; G06F-015/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a secure print system in which security is improved.

SOLUTION: A print server 200 produces unique data in response to receiving of a user name 301 from a host computer 100 and transmits the data to the host computer 100 together with a job ID (302). Besides, a password corresponding to the user name is obtained from a database 400 and encrypted by using the produced unique data to produce an encrypted password, and the encrypted password is paired with the job ID and stored in a database 401. The host computer 100 encrypts the password by using the received unique data and transmits a print job embedded with the obtained encrypted password and the received job ID (303). When the job ID and the encrypted password registered in the database 401 are the same as the job ID and the encrypted password received from the host computer 100, the relevant print job is outputted to a printer 300.

COPYRIGHT: (C)2004,JPO
?

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-308194

(P2003-308194A)

(43) 公開日 平成15年10月31日 (2003. 10. 31)

(51) Int.Cl. ⁷	識別記号	F I	特許出願公開番号 (参考)
G 0 6 F 3/12		C 0 6 F 3/12	K 2 C 1 8 7
B 4 1 J 5/30		B 4 1 J 5/30	Z 5 B 0 2 1
G 0 6 F 15/00	3 3 0	C 0 6 F 15/00	3 3 0 E 5 B 0 8 5

審査請求 未請求 請求項の数22 O L (全 11 頁)

(21) 出願番号 特願2002-113629 (P2002-113629)

(22) 出願日 平成14年4月16日 (2002. 4. 16)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 高木 義博

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 100076428

弁理士 大塚 康徳 (外3名)

Fターム(参考) 2C187 AD03 AD04 AD14 AE07 AE13

BF26 GD02

5B021 AA01 BB04 NN18

5B085 AE03 AE09 AE23 BA07 BG02

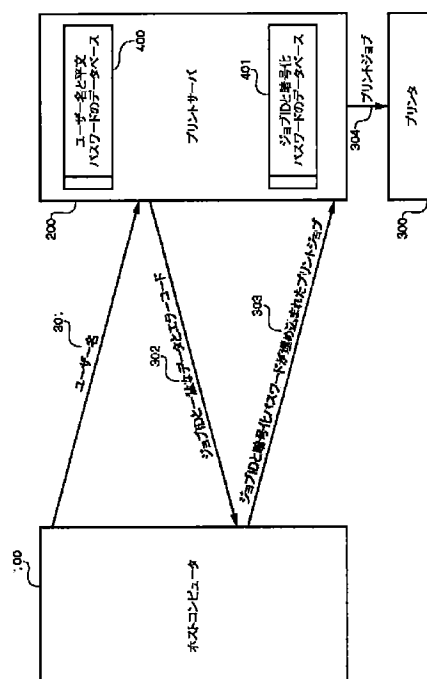
BC07

(54) 【発明の名称】 印刷装置、情報処理装置、プリントサーバ、印刷装置及び印刷システムの制御方法並びに情報処理方法

(57) 【要約】

【課題】セキュリティ性を向上したセキュアプリントシステムを提供する。

【解決手段】プリントサーバ200はホストコンピュータ100からのユーザ名301の受信に応じて一意なデータを生成し、ジョブIDとともにホストコンピュータ100に送信する(302)。また、このユーザ名に対応するパスワードをデータベース400から得て、生成した一意なデータを用いて暗号化して暗号化パスワードを生成し、ジョブIDと対にしてデータベース401に格納する。ホストコンピュータ100は、受信した一意なデータを用いてパスワードを暗号化し、得られた暗号化パスワードと受信したジョブIDを埋め込んだプリントジョブを送信する(303)。データベース401に登録されたジョブIDと暗号化パスワードが、ホストコンピュータ100より受信したジョブIDと暗号化パスワードと同一である場合には、当該プリントジョブをプリンタ300に出力する。



【特許請求の範囲】

【請求項1】 ユーザ名の受信に応じて一意なデータを生成する生成手段と、
前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋めこまれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、
前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブによる印刷を実行させる印刷制御手段とを備えることを特徴とする印刷装置。

【請求項2】 ユーザ名とパスワードを対にして記憶する第1記憶手段を更に備え、
前記暗号化手段は、前記ユーザ名に対応するパスワードを前記第1記憶手段より取得することを特徴とする請求項1に記載の印刷装置。

【請求項3】 受信したユーザ名が前記第1記憶手段に記憶されていない場合に、該ユーザ名の送信元に対してエラーを通知する通知手段を更に備えることを特徴とする請求項1に記載の印刷装置。

【請求項4】 前記生成手段は、前記一意なデータとともにジョブIDを生成し、
前記送信手段は、前記一意なデータとともに前記ジョブIDを前記送信元に送信し、
前記暗号化手段は、前記暗号化パスワードと前記ジョブIDを対にして第2記憶手段に記憶し、
前記比較手段は、前記プリントジョブに埋めこまれた暗号化パスワードとジョブIDの対を、前記第2記憶手段に記憶されている暗号化パスワードとジョブIDの対と比較することを特徴とする請求項1に記載の印刷装置。

【請求項5】 前記印刷制御手段は、前記プリントジョブによる印刷を実行した場合に、前記第2記憶手段に記憶された、当該プリントジョブに対応する暗号化パスワードとジョブIDを消去することを特徴とする請求項4に記載の印刷装置。

【請求項6】 プリントジョブの送信に先立ってユーザ名を送信する第1送信手段と、
前記第1送信手段による送信に応じて受信された一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、
前記暗号化パスワードをプリントジョブに埋め込む埋め込み手段と前記暗号化パスワードの埋め込まれたプリントジョブを送信する第2送信手段とを備えることを特徴とする情報処理装置。

【請求項7】 ユーザ名とパスワードの入力を促すイン

ターフェースを提供することを特徴とする請求項6に記載の情報処理装置。

【請求項8】 前記埋め込み手段は、前記暗号化パスワードと、前記第1送信手段による送信に応じて前記一意なデータとともに受信されたジョブIDとを前記プリントジョブに埋め込むことを特徴とする請求項6に記載の情報処理装置。

【請求項9】 ユーザ名の受信に応じて一意なデータを生成する生成手段と、
前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋めこまれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、
前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブを外部の印刷装置にたいして出力する出力手段とを備えることを特徴とするプリントサーバ。

【請求項10】 ユーザ名とパスワードを対にして記憶する第1記憶手段を更に備え、
前記暗号化手段は、前記ユーザ名に対応するパスワードを前記第1記憶手段より取得することを特徴とする請求項9に記載のプリントサーバ。

【請求項11】 受信したユーザ名が前記第1記憶手段に記憶されていない場合に、該ユーザ名の送信元に対してエラーを通知する通知手段を更に備えることを特徴とする請求項9に記載のプリントサーバ。

【請求項12】 前記生成手段は、前記一意なデータとともにジョブIDを生成し、
前記送信手段は、前記一意なデータとともに前記ジョブIDを前記送信元に送信し、
前記暗号化手段は、前記暗号化パスワードと前記ジョブIDを対にして第2記憶手段に記憶し、
前記比較手段は、前記プリントジョブに埋めこまれた暗号化パスワードとジョブIDの対を、前記第2記憶手段に記憶されている暗号化パスワードとジョブIDの対と比較することを特徴とする請求項9に記載のプリントサーバ。

【請求項13】 前記出力手段は、前記プリントジョブによる印刷を実行した場合に、前記第2記憶手段に記憶された、当該プリントジョブに対応する暗号化パスワードとジョブIDを消去することを特徴とする請求項12に記載のプリントサーバ。

【請求項14】 プリントジョブを発行する第1装置と該プリントジョブを処理する第2装置とを含むシステムであって、

前記第1装置よりプリントジョブの送信に先立ってユーザ名を送信する第1送信手段と、
前記第2装置において前記ユーザ名の受信に応じて一意なデータを生成し、第1装置に送信する第2送信手段と、

前記第1及び第2装置のそれぞれにおいて、前記一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、
前記暗号化パスワードの埋め込まれたプリントジョブを前記第2装置へ送信する第3送信手段と、
前記プリントジョブに埋め込まれた暗号化パスワードと、前記第2装置の前記暗号化手段によって得られた暗号化パスワードを比較する比較手段と、
前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブを出力する出力手段とを備えることを特徴とする印刷システム。

【請求項15】 前記第2装置は外部に印刷装置を接続するプリントサーバであることを特徴とする請求項14に記載の印刷システム。

【請求項16】 前記第2装置は印刷装置であることを特徴とする請求項14に記載の印刷システム。

【請求項17】 ユーザ名の受信に応じて一意なデータを生成する生成工程と、
前記生成工程で生成された一意なデータを前記ユーザ名の送信元に送信する送信工程と、
前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化工程と、
前記一意なデータの送信に応じて受信されたプリントジョブに埋め込まれた暗号化パスワードを抽出し、前記暗号化工程で生成した暗号化パスワードと比較する比較工程と、
前記比較工程により両暗号化パスワードが一致した場合、前記プリントジョブによる印刷を実行させる印刷制御工程とを備えることを特徴とする印刷装置の制御方法。

【請求項18】 プリントジョブの送信に先立ってユーザ名を送信する第1送信工程と、
前記第1送信工程による送信に応じて受信された一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化工程と、
前記暗号化パスワードをプリントジョブに埋め込む埋め込み工程と前記暗号化パスワードの埋め込まれたプリントジョブを送信する第2送信工程とを備えることを特徴とする情報処理方法。

【請求項19】 ユーザ名の受信に応じて一意なデータを生成する生成工程と、
前記生成工程で生成された一意なデータを前記ユーザ名の送信元に送信する送信工程と、

前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化工程と、

前記一意なデータの送信に応じて受信されたプリントジョブに埋め込まれた暗号化パスワードを抽出し、前記暗号化工程で生成した暗号化パスワードと比較する比較工程と、

前記比較工程により両暗号化パスワードが一致した場合、前記プリントジョブを外部の印刷装置にたいして出力する出力工程とを備えることを特徴とする情報処理方法。

【請求項20】 プリントジョブを発行する第1装置と該プリントジョブを処理する第2装置とを含むシステムの制御方法であって、

前記第1装置よりプリントジョブの送信に先立ってユーザ名を送信する第1送信工程と、
前記第2装置において前記ユーザ名の受信に応じて一意なデータを生成し、第1装置に送信する第2送信工程と、

前記第1及び第2装置のそれぞれにおいて、前記一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化工程と、
前記暗号化パスワードの埋め込まれたプリントジョブを前記第2装置へ送信する第3送信工程と、
前記プリントジョブに埋め込まれた暗号化パスワードと、前記第2装置の前記暗号化工程によって得られた暗号化パスワードを比較する比較工程と、
前記比較工程により両暗号化パスワードが一致した場合、前記プリントジョブを出力する出力工程とを備えることを特徴とする印刷システムの制御方法。

【請求項21】 請求項18又は19のいずれかに記載の情報処理方法をコンピュータによって実現するための制御プログラム。

【請求項22】 請求項18又は19のいずれかに記載の情報処理方法をコンピュータによって実現するための制御プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク等を介して複数のユーザが共有して使用する印刷システムに関し、さらに詳しくはいわゆるセキュアプリント機能を有する印刷システムに関するものである。

【0002】

【従来の技術】ネットワーク等を介して複数のユーザが共用して使用するプリンタ装置においては、ユーザ認証による印刷実行の制限を実現する、所謂セキュアプリントを実現するものがある。このセキュアプリントは、一般的には、プリントジョブにユーザ名と平文パスワードもしくは可逆暗号化パスワードを埋め込むことによって実現されている。

【0003】

【発明が解決しようとする課題】そのため次のような問題が発生する。

1. プリントジョブをファイル化して、プリントジョブを解析することでパスワードが簡単に漏洩してしまう。
2. ファイル化したプリントジョブをプリンタへ繰り返し送信することによって、何度でも印刷出来てしまう。

【0004】更に、ネットワーク等を介して複数のユーザが共用して使用するプリンタ装置において、プリンタ装置自体にユーザ認証の機能が無い場合は、セキュアプリントそのものが行えないことが多い。

【0005】本発明は上記課題に鑑みなされたもので、その目的は、セキュリティ性を向上したセキュアプリントシステムを提供可能とすることにある。また、本発明の他の目的は、ファイル化されたプリントジョブを解析してもパスワードの判別を不可能として、セキュリティを向上することにある。また、本発明の他の目的は、プリントジョブが1回しか実行されないようにして、セキュリティの向上を図ることにある。更に、本発明の他の目的は、ユーザ認証機能を持たないプリンタ装置であってもセキュアプリントを実現可能とすることにある。

【0006】

【課題を解決するための手段】上記の目的を達成するための本発明による印刷装置は以下の構成を備える。すなわち、ユーザ名の受信に応じて一意なデータを生成する生成手段と、前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、前記ユーザ名に対応するパスワードを前記一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、前記一意なデータの送信に応じて受信されたプリントジョブに埋め込まれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブによる印刷を実行させる印刷制御手段とを備える。

【0007】また、上記の目的を達成するための本発明による情報処理装置は、プリントジョブの送信に先立ってユーザ名を送信する第1送信手段と、前記第1送信手段による送信に応じて受信された一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、前記暗号化パスワードをプリントジョブに埋め込む埋め込み手段と前記暗号化パスワードの埋め込まれたプリントジョブを送信する第2送信手段とを備える。

【0008】また、上記の目的を達成するための本発明の他の態様によれば、以下の構成を備えるプリンタサーバが提供される。すなわち、ユーザ名の受信に応じて一意なデータを生成する生成手段と、前記生成手段で生成された一意なデータを前記ユーザ名の送信元に送信する送信手段と、前記ユーザ名に対応するパスワードを前記

一意なデータを用いて暗号化し、暗号化パスワードを生成する暗号化手段と、前記一意なデータの送信に応じて受信されたプリントジョブに埋め込まれた暗号化パスワードを抽出し、前記暗号化手段で生成した暗号化パスワードと比較する比較手段と、前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブを外部の印刷装置にたいして出力する出力手段とを備える。

【0009】更に、上記の目的を達成するための本発明による印刷システムは、プリントジョブを発行する第1装置と該プリントジョブを処理する第2装置とを含むシステムであって、前記第1装置よりプリントジョブの送信に先立ってユーザ名を送信する第1送信手段と、前記第2装置において前記ユーザ名の受信に応じて一意なデータを生成し、第1装置に送信する第2送信手段と、前記第1及び第2装置のそれぞれにおいて、前記一意なデータを用いて、前記ユーザ名に対応するパスワードを暗号化し、暗号化パスワードを生成する暗号化手段と、前記暗号化パスワードの埋め込まれたプリントジョブを前記第2装置へ送信する第3送信手段と、前記プリントジョブに埋め込まれた暗号化パスワードと、前記第2装置の前記暗号化手段によって得られた暗号化パスワードと比較する比較手段と、前記比較手段により両暗号化パスワードが一致した場合、前記プリントジョブを出力する出力手段とを備える。

【0010】また、本発明によれば、上記印刷装置、情報処理装置、印刷システムに対応する、印刷処理のための方法が提供される。また、それら方法をコンピュータによって実行させるための制御プログラムも提供される。

【0011】

【発明の実施の形態】以下添付図面を参照して、本発明にかかる実施形態を詳細に説明する。

【0012】＜第1実施形態＞

〔システム構成〕図1は第1実施形態のシステム構成例を示す図である。本実施形態によるセキュアプリント機能は、図1の各ホストコンピュータ100とプリントサーバ200との間で実現される。また、図2は図1のホストコンピュータ及びプリントサーバとプリンタの構成例を示すブロック図である。

【0013】本実施形態のセキュアプリントシステムは、図1に示すように、オペレーティングシステム（以降、OSと表記）による動作環境を提供するホストコンピュータ100と、プリントサーバ200とプリンタ300から構成される。ホストコンピュータ100のOSは、Windows（登録商標）（Microsoft社製）を想定しているがこれに限られるものではない。

【0014】ホストコンピュータ100は、CPU104を備える。CPU104は、ROM105に格納されている基本入出力プログラム（BIOS）に従ってOS（Operating system）プログラムを実行することによ

り、OSを構築するとともに、このOS上で対応するアプリケーションプログラムをRAM106を作業領域として実行して対応する処理を行う。RAM106には、上述のOSプログラム、アプリケーションプログラムおよびその実行に必要なデータがハードディスク装置(HD)103からロードされる。

【0015】ハードディスク装置103には、上述のOSプログラムおよび対応するアプリケーションプログラムが格納されている。なお、本実施形態では、アプリケーションプログラムを格納する記憶装置としてハードディスク装置を用いているが、このハードディスク装置に加えて他の記憶装置例えばFD(フロッピーディスク装置)、CDROM(CDROM読取装置)などを用いて対応するアプリケーションプログラムを格納するように構成してもよい。

【0016】CPU104には、上述のROM105、RAM106とともにKBC(キーボードコントローラ)107、CRTC(ディスプレイコントローラ)108、HDC(ハードディスクコントローラ)109、イーサネット(登録商標)I/F110がCPUバス111を介して接続されている。

【0017】KBC107は、キーボード、マウスなどの入力装置101から入力されたキー信号、指示信号を受け取り、CPUバス111を介してCPU104に伝送するための制御を行う。CRTC108は、CPU104によるアプリケーションの実行結果などをディスプレイ102に表示するための表示制御を行う。HDC109は、ハードディスク装置103へのデータの書込み、読出しを制御する。イーサネットI/F110はイーサネットに接続するためのインターフェースである。第1実施形態では、イーサネットとイーサネットI/F110を介してプリントサーバ200を接続し、このプリントサーバ200との間で所定の通信プロトコルを用いて通信を行う。

【0018】このハードディスク装置103に格納されているアプリケーションプログラムには、印刷制御プログラムが含まれ、これらプログラムをCPU104が読み出して実行することによって印刷制御環境が構築される。印刷制御の詳細については後述する。

【0019】プリントサーバ200の構成において、入力装置201、ディスプレイ202、HD203、CPU204、ROM205、RAM206、KBC207、CRTC208、HDC209、イーサネットI/F210及びCPUバス211の各構成は、ホストコンピュータ100で示した参照番号101~111の各構成と同様のため説明は省略する。

【0020】プリンタ300は、プリントサーバ200のイーサネットI/F210と接続され、プリントサーバ200との間で所定の通信プロトコルを用いて通信を行うためのイーサネットI/F304と、ホストプリン

トサーバ200からイーサネットI/F304を介して入力された指示などに従いROM302に格納されている印刷制御処理、通信制御処理などの制御プログラムを実行するCPU301とを備える。CPU301が制御プログラムを実行する際の作業領域としては、RAM303が用いられる。また、RAM303は画像展開処理のページメモリとしても用いられる。

【0021】CPU301には、上述のROM302、RAM303、イーサネットI/F304とともにバスコントローラI/F305、エンジンI/F306がCPUバス307を介して接続されている。エンジンI/F306は、機構的に画像出力を行うエンジン部308との間でデータおよび信号のやり取りを行う入出力インターフェースであり、エンジンI/F306にはエンジン部308が接続されている。

【0022】[ホストコンピュータ100とプリントサーバ200とプリンタ300との間のデータフロー]図3は、ホストコンピュータ100とプリントサーバ200とプリンタ300との間のデータフローを示す図である。なお、ホストコンピュータ100とプリントサーバ200とプリンタ300との間はイーサネットに接続された状態を示したが、ネットワークを構成するものであれば、USB、IEEE1394、無線LANなど接続形態はなんでもかまわない。

【0023】ホストコンピュータ100からプリントジョブを送信する前にまずユーザ名を含んだデータがホストコンピュータ100からプリントサーバ200へ送信される(301)。それを受けてプリントサーバ200は、エラーコードとジョブIDと一意なデータを送り返す(302)。

【0024】そして、ホストコンピュータ100は、パスワードと一意なデータとに基づいて得られた暗号化パスワードと、上記ジョブIDとを埋め込んだプリントジョブをプリントサーバ200へ送信する(303)。プリントサーバ200においては、上記ジョブIDと暗号化パスワードによる認証を行ない、認証が得られたならばプリントサーバ200はプリンタ300へプリントジョブを送信し印刷を実行する(304)。

【0025】なお、プリントサーバ200は、上記認証を実行するために、ユーザ名と平文パスワードの対で構成されるデータベース400を保持する。このデータベース400は、印刷処理とは独立して管理される。データベースの管理方法としては、ユーザ名から平文パスワードを得られればよく、既存の技術を適用できるので、本実施形態において詳細な説明は省略する。また、プリントサーバ200は、一対のジョブIDと暗号化パスワードから構成されるデータベース401を保持する。このデータベース401の要素データは、印刷処理の実行毎に生成・破棄される。上記認証においては、ホストコンピュータより受信したプリントジョブに埋めこまれて

いるジョブID及び暗号化パスワードと、データベース401に格納されているジョブIDと暗号化パスワードとの比較が行われることになる。

【0026】以上説明した処理をホストコンピュータ100側から説明したフローチャートが図4であり、またプリントサーバ200側から説明したフローチャートが図5である。以降、図4、図5を用いて処理の詳細を説明する。

【0027】[ホストコンピュータ100の処理フロー] ホストコンピュータ100内部の処理を図4に示すフローチャートに従い説明する。

【0028】図4で説明される全ての処理は、ホストコンピュータ100内部で動作するプログラムによって実行される。なお、本実施形態のプログラムの実行形態は、アプリケーション、プリントスプーラ、プリンタドライバ、ランゲージモニタ（処理場プリンタドライバより後段、ポートモニタより前段に位置し、双方向通信を司るモジュールで、デバイスのステータスを取得するのを主要な役割とする）など、様々な形態で実行が可能である。

【0029】印刷処理に先立ち、まずユーザにユーザ名と平文パスワードの入力を促すダイアログボックスを表示し、ユーザ名と平文パスワードを入力させ、これらを得る（ステップS401）。そして、ユーザ名を含んだデータをプリントサーバ200へ送信する（ステップS402）。これはユーザ名のチェックと、ジョブID及び一意なデータの送信要求を意味する。

【0030】ステップS402で送信したユーザ名に対してプリントサーバ200からエラーコードとジョブIDと一意なデータを受信する（ステップS403）。そして、エラーコードによってユーザ名が不正であったかどうかを判定する。なお、ユーザ名が不正な場合は、エラーコードのみが送信されればよく、ジョブIDと一意なデータは送信不要である。

【0031】ジョブIDはホストコンピュータ100で識別可能なデータ形式であればどのような形態であってもかまわない。一般にジョブIDは数値もしくは文字列であることが多い。一意なデータもホストコンピュータ100で識別可能なデータ形式であればどのような形態であってもかまわない。一般に、一意なデータはタイムスタンプから生成される数値や文字列、もしくは、時刻やネットワークカードのMACアドレス（Media Access Control Address）から生成されるGUID（Global Unique ID）などがある。

【0032】エラーコードが不正と判定された場合、即ち不正なユーザであると判定した場合（ステップS404）、不正なユーザである旨の通知を印刷実行者に知らせる（ステップS408）。この通知は、一般にダイアログボックス等を表示することが多い。

【0033】正しいユーザであると判定された場合は、

ステップS401で入手した平文パスワードとステップS403で入手した一意なデータを組み合わせて、これに非可逆の暗号化を施し、暗号化パスワードを得る（ステップS405）。一意なデータを組み合わせることにより印刷実行毎に暗号化パスワードを変化させることができる。なお、非可逆の暗号化処理としては、一般にMD5（Message Digest 5）といったダイジェストアルゴリズムを利用したものが挙げられる。

【0034】続いて、プリントジョブにステップS401で入手したジョブIDとステップS405で生成した暗号化パスワードをプリントジョブに埋め込む（ステップS406）。こうして暗号化パスワードが埋め込まれたプリントジョブをプリントサーバ200へ送信する（ステップS407）。

【0035】[プリントサーバ200の処理フロー] 次に、図3に示したプリントサーバ200内部の処理を図5に示すフローチャートに従い説明する。なお、図5で説明される全ての処理は、プリントサーバ200内部において動作するプログラムによって実行される。

【0036】印刷処理に先立ち、まずホストコンピュータ100からユーザ名が送信されてくる（ステップS501）。受信したユーザ名とデータベース400に登録されているユーザ名を比較することによって、不正なユーザ名かどうかの判定を行う（ステップS502）。不正なユーザ名であると判定されたら、不正なユーザを意味するエラーコードをホストコンピュータ100へ送信して処理を終了する（ステップS512）。

【0037】一方、不正なユーザ名でなければ、ジョブIDと一意な任意のデータを生成する（ステップS503）。上述したように、ジョブIDはホストコンピュータ100で識別可能なデータ形式であればどのような形態であってもかまわない。一般にジョブIDは数値もしくは文字列であることが多い。一意なデータもホストコンピュータで識別可能なデータ形式であればどのような形態であってもかまわない。一般に、一意なデータはタイムスタンプから生成される数値や文字列、もしくは、時刻やネットワークカードのMACアドレス（Media Access Control Address）から生成されるGUID（Global Unique ID）などがある。

【0038】データベース400に登録されていてかつステップS501で受信したユーザ名に対応した平文パスワードと、ステップS503で生成した一意なデータとを組み合わせて、非可逆の暗号化を施し、暗号化パスワードを生成する（ステップS504）。一意なデータを組み合わせることにより印刷実行毎に暗号化パスワードを変化させることができる。なお、この非可逆の暗号化処理は、ホストコンピュータ100において用いられる非可逆暗号化処理（ステップS405）と完全に同じアルゴリズムでなければならない。

【0039】次に、ステップS503で生成したジョブ

IDとステップS504で生成した暗号化パスワードとを関連付けてデータベース401に保存する(ステップS505)。この保存により任意のジョブIDから関連付けられた暗号化パスワードが取得可能になる。

【0040】ステップS501において受信したユーザ名に対する応答として、ステップS503で生成したジョブID及び一意なデータと、成功を意味するエラーコードとをホストコンピュータ100に送信する(ステップS506)。ステップS506によるデータの送信を受けて、ホストコンピュータは図4で説明したようにジョブIDと暗号化パスワードが埋め込まれたプリントジョブを出力する。よって、プリントサーバ200は、ホストコンピュータ100からこのプリントジョブを受信する(ステップS507)。

【0041】このプリントジョブにはジョブIDと暗号化パスワードが埋め込まれているので、これらを取り出し(ステップS508)、ステップS505においてデータベース401に保存しておいたジョブID及び暗号化パスワードと比較する(ステップS509)。

【0042】比較の結果、完全に一致した場合は、プリントジョブをプリンタ300へ送信して印刷を実行し(ステップS510)、ステップS511においてデータベース401に保存しておいた当該ジョブIDと暗号化パスワードを削除する(ステップS511)。このジョブIDと暗号化パスワードの削除により同じプリントジョブを複数回印刷することを妨げることが可能となる。

【0043】以上説明したように第1実施形態によれば、セキュアプリント機能を持たないプリンタ装置であってもセキュアプリントシステムが実現され、さらに、ファイル化されたプリントジョブを解析してもパスワードは判別不可能であり、かつプリントジョブの印刷は1回のみ実行可能となる。

【0044】＜第2実施形態＞第1実施形態ではプリントサーバ200を介してプリンタ300と接続することにより、セキュアプリントの機能を有していないプリンタであっても、セキュアプリントを実行することを可能としている。しかしながら、プリントサーバ200のセキュアプリント機能をプリンタ自身が有する場合には、プリントサーバを介さずにセキュアプリントを実現できる。第2実施形態ではこのようなプリンタについて説明する。

【0045】図6は第2実施形態によるプリンタシステムの構成を示す図である。プリンタ500は共有プリンタとして、プリントサーバを介さずにネットワークに直接に接続されている。

【0046】図7は図6のホストコンピュータとプリンタの構成例を示すブロック図である。ホストコンピュータ100の構成は図2で説明したとおりであるが、第2実施形態では、イーサネットとイーサネットI/F11

0を介してプリンタ500と接続し、プリンタ500との間で所定の通信プロトコルを用いて通信を行なう。

【0047】プリンタ500において、イーサネットI/F504は、ホストコンピュータ100のイーサネットI/F110と接続され、ホストコンピュータ100との間で所定の通信プロトコルを用いて通信を行う。CPU501は、ホストコンピュータ100からイーサネットI/F504を介して入力された指示などに従いROM302に格納されている印刷制御処理、通信制御処理などの制御プログラムを実行する。

【0048】図8は、第2の実施形態によるホストコンピュータ100とプリンタ500との間のデータフローを示す図である。なお、ホストコンピュータ100とプリンタ300との間はイーサネットで接続された状態を示したが、ネットワークを構成するものであれば、USB、IEEE1394、無線LANなど接続形態はなんであって構わない。

【0049】ホストコンピュータ100からプリンタ500へプリントジョブを送信する前にまずユーザ名を含んだデータがホストコンピュータ100からプリンタ500へ送信される(801)。それを受けてプリンタ500は、エラーコードとジョブIDと一意なデータを送り返す(802)。

【0050】そして、ホストコンピュータ100は、パスワードと一意なデータとに基づいて得られた暗号化パスワードと、上記ジョブIDとを埋め込んだプリントジョブを生成し、プリンタ500へ送信する(803)。プリンタ500においては、上記ジョブIDと暗号化パスワードによる認証を行ない、認証が得られたならば当該プリントジョブに対する印刷を実行する。

【0051】なお、第1実施形態で説明したデータベース400、401は、プリンタ500が所有することになる。そして、プリンタ500は、第1実施形態でプリントサーバ200が実行した図5の処理を実行することにより、セキュアプリントを実現するのである。なお、第1実施形態では、図4に示されるホストコンピュータ100の処理はプリントサーバ200に対するものであったが、第2実施形態では、プリンタ500に対する処理となる。

【0052】以上のように第2実施形態によれば、プリントサーバが不要となり、システムの簡易化を達成できる。

【0053】＜他の実施形態＞なお、本発明は、複数の機器(例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど)から構成されるシステムに適用しても、一つの機器からなる装置(例えば、複写機、ファクシミリ装置など)に適用してもよい。

【0054】また、本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体(または記録媒体)を、システムあるい

は装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0055】さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0056】

【発明の効果】以上説明したように、本発明によれば、セキュリティ性を向上したセキュアプリントシステムが提供される。

【図面の簡単な説明】

【図1】第1実施形態のシステム構成例を示す図である。

【図2】図1のホストコンピュータ及びプリントサーバとプリンタの構成例を示すブロック図である。

【図3】ホストコンピュータ100とプリントサーバ200とプリンタ300との間のデータフローを示す図である。

【図4】実施形態によるホストコンピュータの処理を説明するフローチャートである。

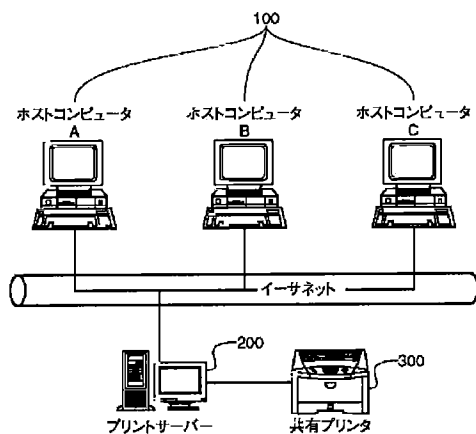
【図5】実施形態によるプリントサーバの処理を説明するフローチャートである。

【図6】第2実施形態によるプリンタシステムの構成を示す図である。

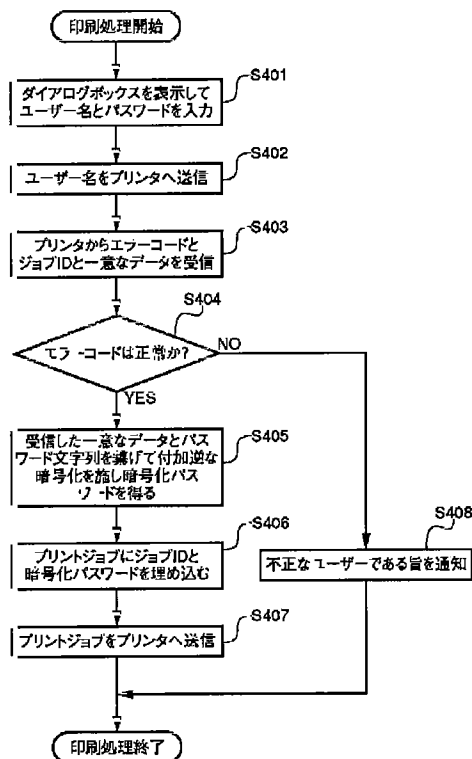
【図7】図6のホストコンピュータとプリンタの構成例を示すブロック図である。

【図8】ホストコンピュータ100とプリンタ500との間のデータフローを示す図である。

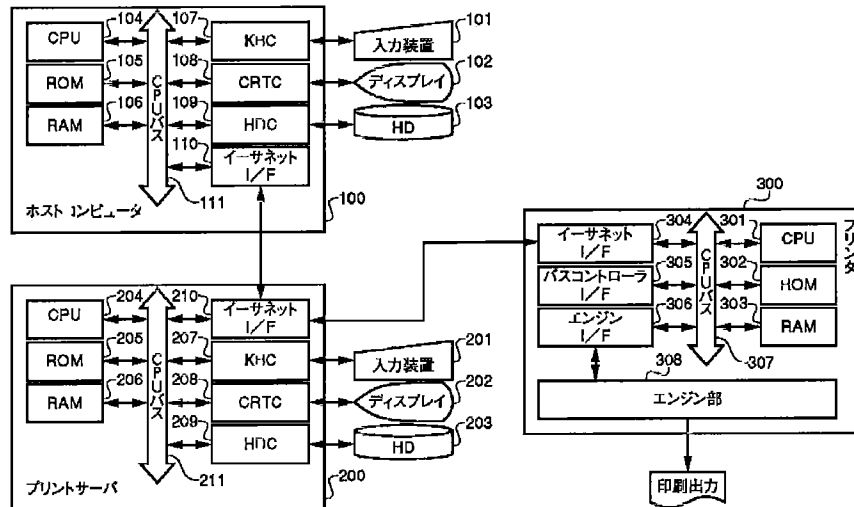
【図1】



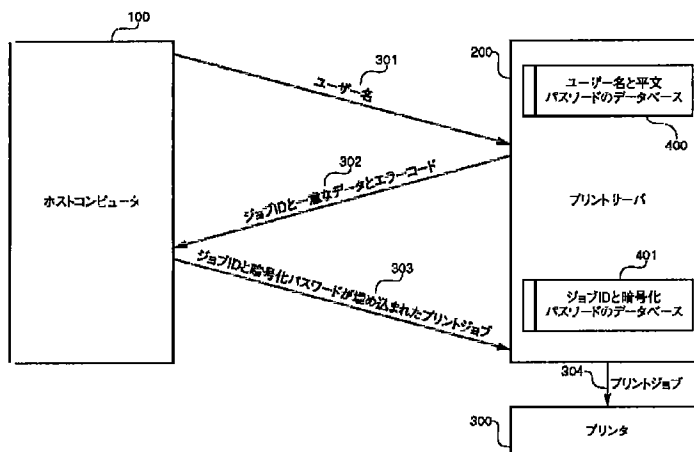
【図4】



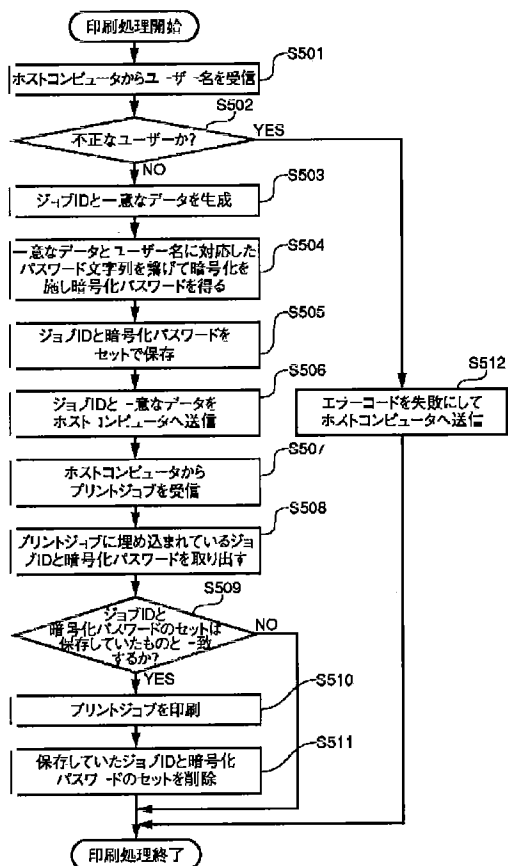
【図2】



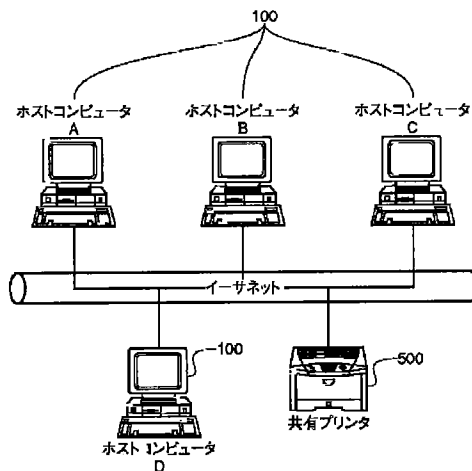
【図3】



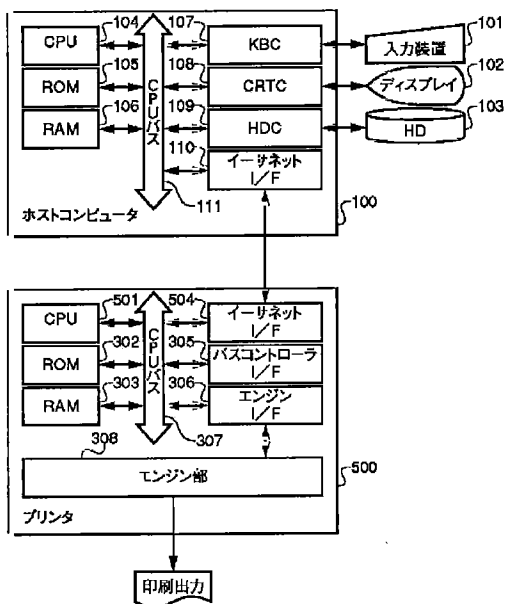
【図5】



【図6】



【図7】



【図8】

